

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

More information about this subseries at <http://www.springer.com/series/7410>

Weizhi Meng · Dieter Gollmann ·
Christian D. Jensen · Jianying Zhou (Eds.)

Information and Communications Security


22nd International Conference, ICICS 2020
Copenhagen, Denmark, August 24–26, 2020
Proceedings

Editors

Weizhi Meng 
Technical University of Denmark
Kongens Lyngby, Denmark

Christian D. Jensen
Technical University of Denmark
Kongens Lyngby, Denmark

Dieter Gollmann
Hamburg University of Technology
Hamburg, Germany

Jianying Zhou 
Singapore University of Technology
and Design
Singapore, Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-61077-7 ISBN 978-3-030-61078-4 (eBook)
<https://doi.org/10.1007/978-3-030-61078-4>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers that were selected for presentation and publication at the 22nd International Conference on Information and Communications Security (ICICS 2020), which was organized by the Cyber Security Section, Technical University of Denmark, Denmark, during August 24–26, 2020. ICICS started in 1997 and aims at bringing together leading researchers and practitioners from both academia and industry to discuss and exchange their experiences, lessons learned, and insights related to computer and communication security. Due to COVID-19, ICICS was held online for the first time.

This year's Program Committee (PC) consisted of 85 members with diverse background and broad research interests. A total of 139 papers were submitted to the conference. The review process was double blind, and the papers were evaluated on the basis of their significance, novelty, and technical quality. Most papers were reviewed by three or more PC members. The PC meeting was held electronically, with intensive discussion over more than one week. Finally, 33 papers were selected for presentation at the conference with an acceptance rate of 23.7%.

After a long discussion among Steering Committee and organization chairs, ICICS 2020 selected two best papers, with a monetary prize generously sponsored by Springer. The paper "A Symbolic Model for Systematically Analyzing TEE-based Protocols," authored by Shiwei Xu, Yizhi Zhao, Zhengwei Ren, Lingjuan Wu, Yan Tong, and Huanguo Zhang, and the paper "Machine Learning based Hardware Trojan Detection using Electromagnetic Emanation," authored by Junko Takahashi, Keiichi Okabe, Hiroki Itoh, Xuan Thuy Ngo, Sylvain Guilley, Ritu Ranjan Shrivastwa, Mushir Ahmed, and Patrick Lejoly, shared the Best Paper Award.

ICICS 2020 had two outstanding keynote talks: "Protecting Your Critical Infrastructure During a Cyber War," presented by Prof. Aditya Mathur from Singapore University of Technology and Design, Singapore, and "End-to-end verifiable e-voting for real-world elections," presented by Prof. Feng Hao from University of Warwick, UK. Our deepest gratitude for their excellent presentations.

For the success of ICICS 2020, we would like to first thank the authors of all submissions and all the PC members for their great efforts in selecting the papers. We also thank all the external reviewers for assisting the review process. For the conference organization, we would like to thank the ICICS Steering Committee, the general chairs, Christian D. Jensen and Jianying Zhou, the publicity chairs, Joaquin Garcia-Alfaro, Qingni Shen, and Bo Luo, and the publication chair, Wenjuan Li. Finally, we thank everyone else, speakers and session chairs, for their contributions to the program of ICICS 2020.

August 2020

Weizhi Meng
Dieter Gollmann

Organization

Steering Committee

Robert Deng	Singapore Management University, Singapore
Dieter Gollmann	Hamburg University of Technology, Germany
Javier Lopez	University of Malaga, Spain
Qingni Shen	Peking University, China
Zhen Xu	Institute of Information Engineering, CAS, China
Jianying Zhou	Singapore University of Technology and Design, Singapore

General Chairs

Christian D. Jensen	Technical University of Denmark, Denmark
Jianying Zhou	Singapore University of Technology and Design, Singapore

Program Chairs

Dieter Gollmann	Hamburg University of Technology, Germany
Weizhi Meng	Technical University of Denmark, Denmark

Publicity Chairs

Joaquin Garcia-Alfaro	Télécom SudParis, France
Qingni Shen	Peking University, China
Bo Luo	University of Kansas, USA

Publication Chair

Wenjuan Li	The Hong Kong Polytechnic University, China
------------	---

Technical Program Committee

Cristina Alcaraz	University of Malaga, Spain
Elena Andreeva	Technical University of Denmark, Denmark
Man Ho Au	The University of Hong Kong, China
Joonsang Baek	University of Wollongong, Australia
Carlo Blundo	Università degli Studi di Salerno, Italy
Xiaofeng Chen	Xidian University, China
Liqun Chen	University of Surrey, UK
Kai Chen	Institute of Information Engineering, CAS, China
Ting Chen	University of Electronic Science and Technology of China, China

Yueqiang Cheng	Baidu USA X-Lab, USA
Songqing Chen	George Mason University, USA
Mauro Conti	University of Padua, Italy
Jintai Ding	University of Cincinnati, USA
Xuhua Ding	Singapore Management University, Singapore
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Joaquin Garcia-Alfaro	Télécom SudParis, France
Xing Gao	University of Memphis, USA
Debin Gao	Singapore Management University, Singapore
Le Guan	University of Georgia, USA
Stefanos Gritzalis	University of the Aegean, Greece
Jinguang Han	Queen's University of Belfast, UK
Shouling Ji	Zhejiang University, China
Chenglu Jin	New York University, USA
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Georgios Kambourakis	University of the Aegean, Greece
Dong Seong Kim	The University of Queensland, Australia
Qi Li	Tsinghua University, China
Shujun Li	University of Kent, UK
Wenjuan Li	The Hong Kong Polytechnic University, China
Xiao Liu	Facebook, USA
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
Xiapu Luo	The Hong Kong Polytechnic University, China
Giovanni Livraga	University of Milan, Italy
Javier Lopez	University of Malaga, Spain
Bo Luo	University of Kansas, USA
Daisuke Mashima	Advanced Digital Sciences Center, Singapore
Jose Maria de Fuentes	Universidad Carlos III de Madrid, Spain
Weizhi Meng	Technical University of Denmark, Denmark
Jiang Ming	The University of Texas at Arlington, USA
Chris Mitchell	Royal Holloway, University of London, UK
Atsuko Miyaji	Osaka University, Japan
Jianbing Ni	University of Waterloo, Canada
Jianting Ning	Singapore Management University, Singapore
Rolf Oppliger	eSECURITY Technologies, Switzerland
Xiaorui Pan	Palo Alto Networks, USA
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Joachim Posegga	University of Passau, Germany
Giovanni Russello	The University of Auckland, New Zealand
Pierangela Samarati	University of Milan, Italy
Nitesh Saxena	University of Alabama at Birmingham, USA
Einar Snekkenes	Norwegian University of Science and Technology, Norway
Qingni Shen	Peking University, China

Vishal Sharma	Singapore University of Technology and Design, Singapore
Chunhua Su	University of Aizu, Japan
Purui Su	Institute of Software, CAS, China
Hung-Min Sun	National Tsing Hua University, Taiwan
Kun Sun	George Mason University, USA
Steve Schneider	University of Surrey, UK
Pawel Szalachowski	Singapore University of Technology and Design, Singapore
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg
Juan Tapiador	Universidad Carlos III de Madrid, Spain
Luca Viganò	King's College London, UK
Shuai Wang	The Hong Kong University of Science and Technology, China
Ding Wang	Nankai University, China
Haining Wang	Virginia Tech., USA
Lingyu Wang	Concordia University, Canada
Weiping Wen	Peking University, China
Zhe Xia	Wuhan University of Technology, China
Christos Xenakis	University of Piraeus, Greece
Jun Xu	Stevens Institute of Technology, USA
Jia Xu	Singtel/Trustwave, Singapore
Zheng Yang	Singapore University of Technology and Design, Singapore
Yu Yu	Shanghai Jiao Tong University, China
Tsz Hon Yuen	The University of Hong Kong, China
Toshihiro Yamauchi	Okayama University, Japan
Junjie Zhang	Wright State University, USA
Tianwei Zhang	Nanyang Technological University, Singapore
Fan Zhang	Zhejiang University, China
Chao Zhang	Tsinghua University, China
Yajin Zhou	Zhejiang University, China
Yongbin Zhou	Institute of Information Engineering, CAS, China

Additional Reviewers

Cong Zuo	Mingli Wu
Yunling Wang	Ruben Rios
Hui Ma	Chao Lin
Tomoaki Mimoto	Eduard Marin
Mohammad Saiful Islam Mamun	Suryadipta Majumdar
Michael Bamiloshin	Arnab Roy
Tomoaki Mimoto	Jose Maria Bermudo Mera
Chenyu Wang	Li Jingwei

Shu Wang
 Carles Angles-Tafalla
 Dongxiao Liu
 Zhichao Yang
 Yanbin Pan
 Xianrui Qin
 Haoyu Ma
 Payton Walker
 Zengrui Liu
 Konstantinos Koutroumpouchos
 Haibo Tian
 Cailing Cai
 Cheng Huang
 Elisavet Konstantinou
 Qilei Yin
 Ashneet Khandpur Singh
 Kent McDonough
 Yue Zhao
 Xiaoyu Zhang
 Ge Wu
 Najeeb Jebreel
 Xin Lou
 Qingqing Ye
 Qiyang Song
 Marios Anagnostopoulos
 Guozhu Meng
 Jianwen Tian
 Hung-Ming Sun
 Cong Wang
 Ahmed Tanvir Mahdad
 Xu Ma
 Kian Hamedani
 Alessandro Visintin
 Hongbing Wang
 Nikolaos Koutroumpouchos
 Shengmin Xu
 Luigi Catuogno
 Aggeliki Tsohou
 Jun Shen
 Yi Wang
 Handong Cui
 Jiageng Chen
 Farnaz Mohammadi
 Marios Anagnostopoulos
 Rami Haffar
 Haoyu Ma

Ankit Gangwal
 Guohua Tian
 Gaurav Choudhary
 Jiageng Chen
 Yunwen Liu
 Qiyang Song
 Prabhakaran Kasinathan
 Weihao Huang
 Ana Nieto
 Yiwen Gao
 Flavio Toffalini
 Xiaoting Li
 Sarah Mccarthy
 Chhagan Lal
 Jianwen Tian
 Guozhu Meng
 Luca Pajola
 Vishakha
 Rodrigo Roman
 Zengpeng Li
 Zhixiu Guo
 Songsong Liu
 Pengbin Feng
 Prabhakaran Kasinathan
 Vaios Bolgouras
 Gaëtan Pradel
 Qingxuan Wang
 Shinya Okumura
 Seungki Kim
 Shengmin Xu
 Elisavet Konstantinou
 Quanqi Ye
 Feng Sun
 Jie Li
 Henrich C. Pöhls
 Yiwen Gao
 Ertem Esiner
 Anna Angelogianni
 Hongbing Wang
 Jiaqi Hong
 Qian Feng
 Vasileios Kouliaridis
 Truan Ho
 Shalini Saini
 Fadi Hassan
 Utku Tefek

Juan Rubio
Christian Berger
Liang Ruigang
Antonio Munoz
Li Jingwei
Yuanyuan He
Korbinian Spielvogel
Yan Lin
Felix Klement
Zengrui Liu

Hung-Ming Sun
Dimitra Georgiou
Luigi Catuogno
Miao Yu
Hoang Minh Nguyen
Jianghong Wei
Jiageng Chen
Huibo Wang
Antonio Munoz

Contents

Security I

Machine Learning Based Hardware Trojan Detection Using Electromagnetic Emanation	3
<i>Junko Takahashi, Keiichi Okabe, Hiroki Itoh, Xuan-Thuy Ngo, Sylvain Guilley, Ritu-Ranjan Shrivastwa, Mushir Ahmed, and Patrick Lejoly</i>	
A Machine Learning-Assisted Compartmentalization Scheme for Bare-Metal Systems	20
<i>Dongdong Huo, Chao Liu, Xiao Wang, Mingxuan Li, Yu Wang, Yazhe Wang, Peng Liu, and Zhen Xu</i>	
Detection of Metamorphic Malware Packers Using Multilayered LSTM Networks	36
<i>Erik Bergenholtz, Emiliano Casalicchio, Dragos Ilie, and Andrew Moss</i>	
Profile Matching Across Online Social Networks	54
<i>Anisa Halimi and Erman Ayday</i>	

Crypto I

A Compact Digital Signature Scheme Based on the Module-LWR Problem.	73
<i>Hiroki Okada, Atsushi Takayasu, Kazuhide Fukushima, Shinsaku Kiyomoto, and Tsuyoshi Takagi</i>	
Tree-Based Ring-LWE Group Key Exchanges with Logarithmic Complexity	91
<i>Hector B. Hougaard and Atsuko Miyaji</i>	
CoinBot: A Covert Botnet in the Cryptocurrency Network	107
<i>Jie Yin, Xiang Cui, Chaojie Liu, Qixu Liu, Tao Cui, and Zhi Wang</i>	
A Symbolic Model for Systematically Analyzing TEE-Based Protocols	126
<i>Shiwei Xu, Yizhi Zhao, Zhengwei Ren, Lingjuan Wu, Yan Tong, and Huanguo Zhang</i>	

Crypto II

New Practical Public-Key Deniable Encryption.	147
<i>Yanmei Cao, Fangguo Zhang, Chongzhi Gao, and Xiaofeng Chen</i>	

A Blockchain Traceable Scheme with Oversight Function	164
<i>Tianjun Ma, Haixia Xu, and Peili Li</i>	
Blind Functional Encryption	183
<i>Sébastien Canard, Adel Hamdi, and Fabien Laguillaumie</i>	
Lattice HIBE with Faster Trapdoor Delegation and Applications	202
<i>Guofeng Tang and Tian Qiu</i>	
Security II	
Attributes Affecting User Decision to Adopt a Virtual Private Network (VPN) App	223
<i>Nissy Sombatruang, Tan Omiya, Daisuke Miyamoto, M. Angela Sasse, Youki Kadobayashi, and Michelle Baddeley</i>	
rTLS: Lightweight TLS Session Resumption for Constrained IoT Devices . . .	243
<i>Koen Tange, David Howard, Travis Shanahan, Stefano Pepe, Xenofon Fafoutis, and Nicola Dragoni</i>	
PiDicators: An Efficient Artifact to Detect Various VMs	259
<i>Qingjia Huang, Haiming Li, Yun He, Jianwei Tai, and Xiaoqi Jia</i>	
HCC: 100 Gbps AES-GCM Encrypted Inline DMA Transfers Between SGX Enclave and FPGA Accelerator	276
<i>Luis Kida, Soham Desai, Alpa Trivedi, Reshma Lal, Vincent Scarlata, and Santosh Ghosh</i>	
Crypto III	
Information-Theoretic Security of Cryptographic Channels	295
<i>Marc Fischlin, Felix Günther, and Philipp Muth</i>	
Client-Oblivious OPRAM	312
<i>Gareth T. Davies, Christian Janson, and Daniel P. Martin</i>	
The Influence of LWE/RLWE Parameters on the Stochastic Dependence of Decryption Failures	331
<i>Georg Maringer, Tim Fritzmann, and Johanna Sepúlveda</i>	
One-Time, Oblivious, and Unlinkable Query Processing Over Encrypted Data on Cloud	350
<i>Yifei Chen, Meng Li, Shuli Zheng, Donghui Hu, Chhagan Lal, and Mauro Conti</i>	

Crypto IV

A New General Method of Searching for Cubes in Cube Attacks	369
<i>Lin Ding, Lei Wang, Dawu Gu, Chenhui Jin, and Jie Guan</i>	
A Love Affair Between Bias Amplifiers and Broken Noise Sources	386
<i>George Teșeleanu</i>	
Towards Real-Time Hidden Speaker Recognition by Means of Fully Homomorphic Encryption	403
<i>Martin Zuber, Sergiu Carpov, and Renaud Sirdey</i>	
A Complete Cryptanalysis of the Post-Quantum Multivariate Signature Scheme Himq-3	422
<i>Jintai Ding, Zheng Zhang, Joshua Deaton, and Lih-Chung Wang</i>	

Security III

Statically Dissecting Internet of Things Malware: Analysis, Characterization, and Detection	443
<i>Afsah Anwar, Hisham Alasmay, Jeman Park, An Wang, Songqing Chen, and David Mohaisen</i>	
Analysis of Industrial Device Architectures for Real-Time Operations Under Denial of Service Attacks	462
<i>Florian Fischer, Matthias Niedermaier, Thomas Hanka, Peter Knauer, and Dominik Merli</i>	
A Variational Generative Network Based Network Threat Situation Assessment	479
<i>Hongyu Yang, Renyun Zeng, Fengyan Wang, Guangquan Xu, and Jiyong Zhang</i>	

Crypto V

A Hardware in the Loop Benchmark Suite to Evaluate NIST LWC Ciphers on Microcontrollers	495
<i>Sebastian Renner, Enrico Pozzobon, and Jürgen Mottok</i>	
Experimental Comparisons of Verifiable Delay Functions	510
<i>Zihan Yang, Bo Qin, Qianhong Wu, Wenchang Shi, and Bin Liang</i>	
Attacks on Integer-RLWE	528
<i>Alessandro Budroni, Benjamin Chetoui, and Ermes Franch</i>	

A Family of Subfield Hyperelliptic Curves for Use in Cryptography	543
<i>Anindya Ganguly, Abhijit Das, Dipanwita Roy Chowdhury, and Deval Mehta</i>	
 Crypto VI	
Leakage-Resilient Inner-Product Functional Encryption in the Bounded- Retrieval Model	565
<i>Linru Zhang, Xiangning Wang, Yuechen Chen, and Siu-Ming Yiu</i>	
Anonymous End to End Encryption Group Messaging Protocol Based on Asynchronous Ratchet Tree	588
<i>Kaiming Chen and Jiageng Chen</i>	
Author Index	607